Symantec™ Endpoint Protection Integration Component 7.5 Release Notes

Symantec™ Endpoint Protection Integration Component 7.5 Release Notes

Legal Notice

Copyright © 2013 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark LogoAltiris, and any Altiris or Symantec trademarks used in the product are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information

- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Endpoint Protection Integration Component

This document includes the following topics:

- About Endpoint Protection Integration Component
- System requirements
- Supported Antivirus solutions
- General installation and upgrade information
- Known issues
- Fixed issues
- Other things to know

About Endpoint Protection Integration Component

Endpoint Protection Integration Component facilitates migration to Symantec Endpoint Protection through robust software delivery mechanisms. The software provides detailed reporting, broad deployment views (dashboards), bandwidth throttling, and advanced discovery. This free component can scale for both local and remote endpoints.

Endpoint Integration Component combines Symantec Endpoint Protection with your other Symantec Management Platform based products. You can inventory computers, deliver software and patches, and deploy new computers. You can also back up and restore your systems and data, manage data loss prevent (DLP) agents, and manage Symantec Endpoint Protection clients. You can do this work from a single, Web-based Symantec Management Console.

System requirements

Endpoint Protection Integration Component requires the following software to be installed:

- Symantec Management Platform 7.5.
  When you install Endpoint Protection Integration Component using Symantec Installation Manager, the Symantec Management Platform is installed automatically.
- Symantec-Real Time Console Infrastructure 7.5.

The operating systems that are supported by the Symantec Management Platform are also supported by Endpoint Protection Integration Component.

For more information, see the product support matrix at the following URL:
http://www.symantec.com/docs/HOWTO9965

Supported Antivirus solutions

Endpoint Protection Integration Component 7.5 supports the following antivirus solutions:

- ESET NOD32 Anti-Virus 6.0.308/3.0/4.0/4.2/Korean 4.2/Chinese Simple 4.0, 4.2/ Chinese Traditional 4.0, 4.2 (Chinese Simplified, Chinese Traditional, English, and Korean)
- McAfee 8.7/12.1
- Trend Micro Office Scan 8.3/10.0/10.5/10.6 SP2
- F-Secure Anti-Virus for Windows Servers 8.01/9.00/9.50
- F-Secure Windows Client 8.00/9.01
- F-Secure Anti-Virus/Internet Security 1.77.243
- CA Anti-Virus 7.00
- SOPHOS Endpoint Security and Control 7.6.4/9.0
- SOPHOS Anti-Virus 9.5/10.0.7
- Symantec Anti-Virus 8.11/10.1/10.2
- Kaspersky Anti-Virus 6.0.4.1212/11.01.400/13.0.1.4190
- Microsoft Forefront endpoint protection 2.0.657
- Microsoft client security 1.5.1937.3

Note: You must have at least one of the antivirus solutions installed on the client computer to migrate successfully.

General installation and upgrade information

You install the Symantec Management Platform (SMP) 7.5 and the Symantec Endpoint Protection Integration Component (SEPIC) using Symantec Installation Manager.

Installation of Symantec Management Platform 7.5 and the SEPIC 7.5

You can download the installation files directly to your server or you can create offline installation packages.

For more information on how to install and configure the product, see the Installing the IT Management Suite solutions chapter in the *IT Management Suite 7.5 Installation and Upgrade Guide* at the following URL:

http://www.symantec.com/docs/DOC5697

Upgrade to Symantec Management Platform 7.5 and the SEPIC 7.5

To perform an upgrade from version 7.1 or later, in the Symantec Installation Manager click **Install New Products**, and then choose to install this product. Do not use the **Install Product Updates** page to upgrade.

For more information about the latest updates in the Symantec Management Platform, refer to the *Symantec Management Platform 7.5 Release Notes* at the following URL:

http://www.symantec.com/docs/DOC6713

The supported upgrade paths to SEPIC 7.5 from the earlier release versions to the latest release version are as follows:

Table 1-1 Supported upgrade paths to SEPIC 7.5

Solution	Supported upgrade paths
SEPIC	■ 7.1 SP1/ SP1b ■ 7.1 SP2/ R v4 ■ 7.1 SP2 MP1.1

For more information on how to upgrade to SEPIC 7.5, see the Upgrading to IT Management Suite 7.5 chapter in the *IT Management Suite 7.5 Installation and Upgrade Guide* at the following URL:

http://www.symantec.com/docs/DOC5697

Upgrade to Symantec Management Agent 7.5

After upgrade to SMP 7.5 and SEPIC 7.5, you must upgrade the Symantec Management Agent (SMA) on client computers to SMA 7.5. Additionally, you must upgrade the SMA plug-ins to the latest versions that are available in SMP 7.5 and SEPIC 7.5. Different versions of the SMA and plug-ins are not supported in 7.5 release.

To upgrade to Symantec Management Agent 7.5, you can execute any one of the following tasks:

- In the Symantec Management Console, click **Actions > Agents/Plug-ins > Rollout Agents/Plug-ins**. Then, in the left pane, under **Symantec Management Agent**, locate and turn on the upgrade policies for the Symantec Management Agent.
- In the Symantec Management Console, click **Settings > All Settings**. In the left pane, expand **Notification Server > Site Server Settings**, and then locate and turn on the upgrade policies for various site server plug-ins.
- In the Symantec Management Console, click **Actions > Agents/Plug-ins > Rollout Agents/Plug-ins**. Then, in the left pane, locate and turn on the upgrade policies for various plug-ins.

Symantec recommends that you configure a schedule for these policies; the default **Run once ASAP** option may not trigger the policy if this is not the first time you perform an upgrade. Also, to speed up the upgrade process, consider temporarily changing the **Download new configuration every** setting on the **Targeted Agent Settings** page to a lower value.

For detailed instructions on migrating from 6.x or 7.0 to 7.5, see the following documentation resources:

- *IT Management Suite Migration Guide version 6.x to 7.5* at the following URL: http://www.symantec.com/docs/DOC5668
- *IT Management Suite Migration Guide version 7.0 to 7.5* at the following URL: http://www.symantec.com/docs/DOC5669

Known issues

The following are the known issues for this release:

Table 1-2 Known issues

Issue	Description
Collecting Antivirus Inventory for F-Secure Anti-Virus 2012	The **Antivirus inventory** task is unable to collect inventory for F-Secure Anti-Virus 2012.
Support for McAfee 2011 v10.5.227 in JP/CS/CH/KN languages	Endpoint Protection Integration Component does not support McAfee 2011 in the following languages: ■ Chinese Simplified ■ Japanese ■ Korean ■ Chinese Traditional
Endpoint Protection Integration Component task issues with Symantec Endpoint Protection 12.1	Endpoint Protection Integration Component scan tasks such as full scan and Quick Scan fail on Symantec Endpoint Protection 12.1.
Endpoint Protection Integration Component repair task execution	Endpoint Protection Integration Component repair task does not execute for the supported Symantec Endpoint Protection versions except Symantec Endpoint Protection 11.0.7072.1031.
Registry entries and folders	Few registry entries and folders are present even after you uninstall the existing antivirus. The count of these entries and folders varies for the antivirus solutions.

Table 1-2 Known issues *(continued)*

Issue	Description
Uninstallation and inventory of localized antivirus software	The Endpoint Protection Integration Component 7.5 does not support inventory or uninstallation of the localized versions of the following antivirus software: ■ F-Secure AV 2012 ■ F-Secure IS 2012 ■ F-Secure AV for workstations 9.30 ■ Kaspersky Endpoint Protection Integration Component 7.5 by default supports the uninstallation and inventory of the following localized antivirus software: ■ ESET NOD32 5.0 ■ ESET SMART SECURITY 5.0 ■ CA Antivirus Plus 2010 ■ McAfee Antivirus Plus 2012 ■ McAfee Total Protection 2012 ■ Trend Micro Office Scan Client 10.5 ■ F-Secure AV for Windows Servers 9.20 ■ SAVCE 10.1.9000.1 ■ SOPHOS Antivirus 9.7 Endpoint Protection Integration Component 7.5 supports the uninstallation of the following localized antivirus software: ■ MS Forefront Endpoint Protection 2010 ■ SAVCE 10.1.9000.9
32-bit and 64-bit package	If a 32-bit package is selected for installation on a 64-bit computer, or a 64-bit package is selected for installation on a 32-bit computer, then the migration job fails.
Power Sensitive Malware Scanning and Remote Machine Repair via IDER and SERT tasks are not supported on CEM environment.	The **Power Sensitive Malware Scanning** and Remote Machine Repair via IDER and SERT tasks do not work in CEM environment as the **Power On** task is not supported on the CEM environment.
Support for uninstallation of Kaspersky Antivirus	The Symantec Endpoint Protection Integration Component 7.5 does not support the uninstallation of Kaspersky antivirus.

Fixed issues

The following are the fixed issues for this release:

Table 1-3 Fixed Issues

Issue	Description
The pie chart legend summary displayed incorrect client computer numbers.	The pie chart legend summary of the managed, unmanaged, unprotected, and managed protected computers displayed incorrect client computer numbers. This issue has been fixed.
The SEPIC migration job succeeded when the CA Antivirus Plus v2.0.0.265 and the CA Internet Security Suit 6.0.0.285 were installed on the client computer.	The SEPIC migration job succeeded when the CA Antivirus Plus v2.0.0.265 and CA Internet Security Suit 6.0.0.285 were installed on the client computer. This issue has been fixed.
SEPIC used all resources instead of all computers as resource targets.	The Endpoint Protection Integration used all resources instead of all computers as resource target. This issue has been fixed.
Notification Server web applications had the view state MAC disabled.	Notification Server web applications had the view state MAC disabled and was a security threat. This issue has been fixed.
Endpoint Protection Integration failed to uninstall ESET-NOD32 Ver4.0, after installing SEP Client on the client computer.	The Endpoint Protection Integration failed to uninstall ESET-NOD32 Ver4.0, after installing SEP Client on the client computer. This issue has been fixed.
The SEPIC 7.1.1037 - RTCI security privileges were changed during SEPIC configuration.	The SEPIC 7.1.1037 - RTCI security privileges were changed during SEPIC configuration. This issue has been fixed.
The **System Jobs and Task contents** did not display the description about Symantec Endpoint Protection Management.	The **System Jobs and Task contents** did not display description about Symantec Endpoint Protection Management This issue has been fixed.
The Endpoint Protection Integration task issue on delivery of the SEP 12.1 package to the client computers.	The Endpoint Protection Client Integration Migration task failed to delivery of SEP12.1 package on the client computers which had ESET NOD 32 antivirus installed. This issue has been fixed.

Table 1-3 Fixed Issues *(continued)*

Issue	Description
Installation of SEP 12 RU1 failed on client computers installed with SOPHOS 9.5.	The installation of SEP12 RU1 failed on client computers that are installed with SOPHOS 9.5 This issue has been fixed.
The SEP installation failed on client computers where McAfee 2011 was installed.	The SEP installation failed during migration of SEP12 RU1 package on client computers installed with McAfee 2011. This issue has been fixed.

Other things to know

Following are things to know about this release.

- Deprecated features
  See Table 1-4 on page 13.
- Things to know
  See Table 1-5 on page 13.
- Technology: Wake-on-LAN option or Intel vPro option
  See Table 1-6 on page 14.
- Testing results for multiple vPro scenarios
  See Table 1-7 on page 15.

Table 1-4 Deprecated features

Issue	Description
The **Repair Symantec Endpoint Protection Client** task does not support SEP 12.1 onwards.	The repair capability in SEPIC is limited to supported SEP versions older than 12.0. This capability is not available for newer versions

Table 1-5 Things to know

Issue	Description
Remote SERT Boot Task : IDER takes time to boot depending on size of an image	After you perform an IDE-Redirection, the vPro client takes some time to boot depending on the size of the image. There is no progress indicator provided on the **Remote SERT Boot Task** page. Once the restart is done, you can connect to the remote computer through the pcAnywhere **Remote Control** button. This could be verified if you try to connect to the vPro client immediately after redirection and if you are not able to connect to the client computer. This issue indicates that the client computer is in booting state.

Table 1-5 Things to know *(continued)*

Issue	Description
Remote SERT Boot Task : IDER is performed only on one computer at a time	The **Remote SERT Boot Task** is performed only on one computer at a time. If you select multiple computers, the redirection operation is performed on all the computers although you can take remote control of only one computer at a time. The Stop Redirection operation is performed on all the selected vPro computers
Power Sensitive Malware Scanning: Power On task fails on Wake-on-LAN enabled computers	Since the **Power On** task is designed for vPro computers, the task is expected to fail on non-vPro Wake-on-LAN enabled computers. The job continues to the next Wake-on-LAN task, which turns on non-vPro computers. The Wake-on-LAN task succeeds on vPro computers
Default connection profile should be configured before you execute **Remote SERT Boot Task** and **Power Sensitive Malware Scanning** Job	Before executing **Remote SERT Boot Task** and **Power Sensitive Malware Scanning** Job, you must configure the Default connection profile pertaining to the vPro computer's credentials (AMT protocol in Edit Default connection profile Window), so that the tasks execute successfully on vPro clients.
Default connection profile should be selected while executing **Remote SERT Boot Task** and **Power Sensitive Malware Scanning** Job.	When you create a **Remote SERT Boot Task** instance or **Power Sensitive Malware Scanning** Job instance, you should select the Default connection profile which has been configured for use on vPro computers. **Note:** For the **Power Sensitive Malware Scanning** Job, AMT credentials for all selected vPro computers must be the same.
Viewing the summary of unmanaged, managed unprotected and managed protected computers	The information pertaining to view the unmanaged, managed unprotected, and managed protected computers report was not incorporated in the User Guide. Do the following to view the summary of unmanaged, managed unprotected, and managed protected computers 1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**. 2 In the left pane, click **Reports > Symantec Endpoint Protection Management > Details of unmanaged, managed unprotected and managed protected computers**.

The timeouts that are defined for each task in the Power Sensitive Malware are as follows:

Table 1-6 Technology: Wake-on-LAN option or Intel vPro option

Task	Hours
Wake on LAN/Power On (vPro)	60 mins /Approximately 1 hr

Table 1-6 Technology: Wake-on-LAN option or Intel vPro option *(continued)*

Task	Hours
Update Antivirus Definition	30 mins
Quick Scan /Full scan	60 min/10 hrs
Power off	30 mins

The results of the tests for multiple vPro scenarios are as follows:

Table 1-7 Testing results for multiple vPro scenarios

Type of scan	Scenario	Result
Power Sensitive Malware Scan	Select Both technologies (vPro and Wake On LAN) and execute a job on multiple computers (WOL and vPro), keeping one or more vPro computers unplugged.	Success. Job continues in other plugged computers.
Power Sensitive Malware Scan	Select Both technologies and execute a job on multiple computers (WOL and vPro), keeping one or more WOL computers unplugged.	Success. Job continues in other plugged computers.
Power Sensitive Malware Scan	Select Both technologies and execute a job on multiple computers (vPro only), keeping one or more vPro computers unplugged.	Success. Job continues in other plugged computers.
Power Sensitive Malware Scan	Select Both technologies and execute a job on multiple computers (WOL only), keeping one or more WOL computers unplugged.	Success. Job continues in other plugged computers.
Remote SERT Boot Task	Execute a task on Multiple vPro computers.	IDER task does not work on multiple vPro computer. It is designed for single vPro computer.

Table 1-7 Testing results for multiple vPro scenarios *(continued)*

Type of scan	Scenario	Result
Remote SERT Boot Task	Execute a task on Multiple vPro computers and stop IDER by clicking on Stop Redirection button.	Stop Redirection functionality does not work on multiple vPro computer. But it works for single redirected vPro computer.